UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/816,756 | 04/02/2004 | Kok Wai Chan | MS#307522.01 (5108) | 1127 |

38779 7590 09/11/2007

SENNIGER POWERS (MSFT)
ONE METROPOLITAN SQUARE, 16TH FLOOR
ST. LOUIS, MO 63102

| EXAMINER | |
|---|---|
| HENEGHAN, MATTHEW E | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 09/11/2007 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@senniger.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/816,756 | CHAN ET AL. | |
| | Examiner | Art Unit | |
| | Matthew Heneghan | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *02 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 April 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5 IDS's*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-32 have been examined.

### *Information Disclosure Statement*

2. The following Information Disclosure Statements in the instant application have been fully considered:

IDS filed 2 April 2004.

IDS filed 7 June 2004.

IDS filed 10 January 2006.

IDS filed 19 April 2006.

IDS filed 20 December 2006.

### *Drawings*

3. The drawings are objected to because:

Arrows appear to be missing linking items 702, 704, and 706 together in figure 7.

The word "encrypted" is misspelled in item 710, the word "access" is misspelled in item 809, and the word "server" is misspelled in item 904.

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "422" has been used to designate two different encryptions in figure 4.

5. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: items 308, 314, 419, 500, 600, and 907.

6. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: items 100 and 224.

7. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### *Specification*

8. The use of the trademark RC4 has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

9. The disclosure is objected to because of the following informalities: A reference is made in paragraph 39 to Figure 2A, which does not exist.

Appropriate correction is required.

10. The abstract of the disclosure is objected to because in lines 10-11, the phrase "... to retrieve encrypted private from the server..." appears to be missing a word. Correction is required. See MPEP § 608.01(b).

### *Claim Objections*

11. Claim 28 is objected to because of the following informalities: On p. 29, line 1, the word "retrieved" is misspelled. Appropriate correction is required.

### *Claim Rejections - 35 USC § 101*

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

12. Claims 11, 21-24, 31, and 32 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The claims are recited as being embodied on computer-readable media; Applicant's specification specifies that the term "computer-readable medium" encompasses intangible communications media such as carrier waves (see paragraph 61). The claims are therefore non-statutory.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

13. Claims 25-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 25 recites the limitation "the wrapping key" in the last line. There is insufficient antecedent basis for this limitation in the claim. It is being presumed that this

refers to the function of an encryption password unknown to the server as recited in the third limitation.

Claims 26-30 depend from rejected claim 25, and include all the limitations of that claim, thereby rendering those dependent claims indefinite.

***Claim Rejections - 35 USC § 102 and 35 USC § 103***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 1-4, 11-15, 21-24, 31, and 32 are rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over U.S. Patent No. 6,160,891 to Al-Salqan.

As per claims 1, 2, and 12-14, Al-Salqan discloses a system implemented on one or more computers ("each computer system", see column 3, line 48), which must be

networked, in which an inputted key is stored in a local storage (see column 3, lines 65-66). The system encrypts it using a symmetric function (the wrapping key, which may be derived from a password, see column 3, line 59 and column 6, lines 25-28) (see column 4, lines 47-52). After an additional asymmetric encryption, using one of a public/private key pair (the recovery keys), the encrypted value is sent to key recovery file storage which may be at a certificate authority, which inherently comprises a server, see column 5, lines 21-24) (see column 4, line 62 to column 5, line 5 and column 5, lines 50-52). An attempt to retrieve (i.e. a request) for the encrypted key may then be received at the trusted authority (see column 5, lines 46-47), which sends the encrypted key back to the client (see column 5, lines 25-35). Since this may be sent to "another party" (see abstract; column 7, lines 7-10), this is a second client.

Though the key recovery file storage is clearly at a server, it is unclear whether the clients are inherently connected via a data communications network to the server.

Official notice is given that it is well-known in the art to assign each individual user at least one client computer in such systems.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Al-Salqan using client computers for each user.

As per claims 3 and 15, at the decryption end, private information is required from the user (see column 5, lines 36-44). The symmetric decryptor uses the private information gathered and decrypts as per the encryption method. Since the encryption

used a password input, the decryption must also use a password input (see column 6, lines 38-52).

As per claim 4, the user's public key may be used in public/private key transactions (see column 6, line 10); in this scenario, the client encrypts with the user's private key (the "private data"), which is also the recovery key, and the server decrypts it with the user's corresponding public key; therefore the client sends the server the recovery key wrapped by the symmetric key. The private information that comprises the symmetric key must be passed to storage (at the server) (see column 5, lines 50-67) as part of the transmission to the server under the recovery key). The prompting of the user for information (see column 4, lines 8-9) constitutes a recovery option being selected by a user.

As per claims 11, 21-24, 31, and 32, Al-Salqan's invention may be embodied on computer-readable media (see column 3, lines 41-47).

15. Claims 10 and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,160,891 to Al-Salqan.

Regarding claim 10, Al-Salqan does not specify whether the second client should be at a fixed or a roaming client.

Official notice is given that it is well-known in the art to deploy clients at roaming workstations, in order to allows users the ability to user their systems to access the system anywhere in a facility.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a roaming client for the second client, in order to allows users the ability to user their systems to access the system anywhere in a facility.

As per claims 25-27, Al-Salqan discloses that key recovery information may be retrieved after a user supplies identity verification information (see column 6, lines 14-22) and that such information may be a hashed password (see column 4, lines 29-44).

16. Claims 5-9, 16-20, and 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,160,891 to Al-Salqan as applied to claim 1 et al. above, and further in view of Maher, "Crypto Backup and Key Escrow," Communications of the ACM, Volume 39, Issue 3, pp. 48-53, 1996.

Regarding claims 5 and 16, though Al-Salqan's invention is oriented towards recovering systems in the event of a lost password (see abstract), Al-Salqan does not disclose the issuing of a backup key.

Maher discloses the analogous use of backup keys, in which a server (Bob) generates and issues to a user (Alice) a public MasterKey vector as part of the key archiving operation. Bob keeps a copy of the vector (in server storage), which Alice then incorporates into her key generator (see first System Scenario on p. 49).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Al-Salqan by using Maher's backup key system to further aid in the recovery keys after a lost password.

It would be obvious, then, for Alice to use this key to encrypt and store her keys, including her recovery keys.

Regarding claim 6, in a recovery operation under Al-Salqan in view of Maher, key information sent to a client by a server would be further encrypted under the public backup key issued by the server. The sending of the encrypted recovery and backup keys to the client by the server would be essential to any key recovery attempt at a client.

Regarding claims 7-9, 19, 20, and 28-30, since Al-Salqan provides that the keys should also be recoverable by "another party," it would be obvious to issue support all functionalities and issue all of the necessary key recovery information to a second client.

Regarding claims 17 and 18, Maher's modification includes the use of a random number in key generation (see p. 50, second column, step 2).

## *Conclusion*

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is

(571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand, can be reached at (571) 272-3811.

**Any response to this action should be mailed to:**
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
**Or faxed to:**
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Matthew Heneghan/

September 3, 2007

Patent Examiner (FSA), USPTO Art Unit 2134